A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTIONS

ABSTRACT OF THE DISCLOSURE

An electronic transaction system, which facilitates secure electronic transactions among multiple parties including cardholders, merchants, and service providers (SP). The system involves electronic cards, commonly known as smart cards, and their equivalent computer software package. The card mimics a real wallet and contains commonly seen financial or non-financial instruments such as a credit card, checkbook, or driver license. A transaction is protected by a hybrid key cryptographic system and is normally carried out on a public network such as the Internet. Digital signatures and challenges – responses are used to ensure integrity and authenticity. The card utilizes secret keys such as session keys assigned by service providers (SPs) to ensure privacy for each transaction. The SP is solely responsible for validating each participant's sensitive information and assigning session keys. The system does not seek to establish a trust relationship between two participants of a transaction. The only trust relationship needed in a transaction is the one that exists between individual participants and the SP. The trust relationship with a participant is established when the SP has received and validated certain established account information from that particular participant. To start a transaction with a selected SP, a participant must have the public key of the intended SP. Since the public key is openly available, its availability can be easily established by the cardholder. The SP also acts as a gateway for the participants when a transaction involves interaction with external systems.

AH/ah

#184297v2